UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TENNESSEE
AT KNOXVILLE

| | | |
|---|---|---|
| UNITED STATES OF AMERICA, | ) | |
| | ) | |
| Plaintiff, | ) | |
| | ) | 3:16-CR-35 |
| v. | ) | |
| | ) | JUDGES JORDAN/SHIRLEY |
| THOMAS ALLAN SCARBROUGH, | ) | |
| also known as "Teddybear555," | ) | |
| | ) | |
| Defendant. | ) | |

**RESPONSE TO DEFENDANT'S MOTION TO SUPPRESS**

The United States of America by and through the Acting United States Attorney hereby responds to defendant's Motion to Suppress (Doc. 14) (hereinafter "defendant's Motion") as follows. For the reasons set forth herein, the defendant's Motion should be denied.

## I. INTRODUCTION

The search warrant issued for the defendant's residence was largely predicated upon the results of an FBI investigation into a website dedicated to the sharing of child pornography known as "Playpen." The FBI had sought and obtained a warrant permitting it to deploy a "Network Investigative Technique" (the "NIT") that would cause a computer logging into Playpen to reveal certain identifying information—most importantly, its concealed Internet Protocol ("IP") address.

The affidavit supporting the NIT Warrant Application (included within Attachment 1 hereto) established the need for the NIT to identify Playpen users and set forth ample probable cause to conclude that any users Playpen knew of its illicit content and intended to access that content. As the affidavit explained, Playpen was no ordinary website but a hidden site operating on an anonymous network that was dedicated to the sharing of child pornography. The

magistrate judge reasonably concluded that there was a fair probability that anyone who logged into Playpen did so with knowledge of its content and intent to view that content.

Among the IP addresses identified accessing Playpen was one belonging to the defendant. Following the execution of the search warrant at the defendant's residence and the forensic examination of the defendant's computer, the defendant was indicted for distributing child pornography and possessing child pornography involving a prepubescent minor or minor that had not attained the age of 12. (Doc. 3).

## II. THE NIT WARRANT WAS LEGALLY APPROPRIATE

### A. Overview of the Warrants Leading to the Indictment

As described in the 31-page affidavit in support of the NIT Warrant ("NIT Affidavit"), the affiant was a veteran FBI agent with 19 years of federal law enforcement experience and particular training and experience investigating child pornography and the sexual exploitation of children. NIT Affidavit ¶ 1. The NIT Affidavit clearly and comprehensively articulated probable cause to deploy the NIT to obtain IP address and other computer-related information that would assist law enforcement in identifying registered Playpen users who were utilizing the Tor's anonymization technology to expose child sexual exploitation on a massive scale.

Because of the technical and legal complexity of the investigation, the NIT Affidavit included a three-page explanation of the offenses under investigation, a seven-page section providing definitions of technical terms therein, and a three-page description of the Tor. NIT Affidavit ¶¶ 4-10. The NIT Affidavit specified the numerous steps that a Playpen user would have to take in order to find Playpen because it was a Tor hidden service, not an ordinary public website. In particular, the NIT Affidavit noted that:

> Even after connecting to the Tor network, however, a user must know the web address of the website in order to access the site. Moreover, Tor hidden services

> are not indexed like websites on the traditional Internet. Accordingly, unlike on the traditional Internet, a user may not simply perform a Google search for the name of the website on Tor to obtain and click on a link to the site. A user might obtain the web address directly from communicating with other users of the board, or from Internet postings describing the sort of content available on the website as well as the website's location. For example, there is a Tor "hidden service" page that is dedicated to pedophilia and child pornography. That "hidden service" contains a section with links to Tor hidden services that contain child pornography. The TARGET WEBSITE is listed in that section. Accessing the TARGET WEBSITE therefore takes numerous affirmative steps by the user, making it extremely unlikely that any user could simply stumble upon the TARGET WEBSITE without understanding its purpose and content.

*Id.* ¶ 10.

The NIT Affidavit also described the website whose users were targeted by the investigative technique. It described that Playpen was "dedicated to the advertisement and distribution of child pornography," "discussion of … methods and tactics offenders use to abuse children," and "methods and tactics offenders use to avoid law enforcement detection while perpetrating online child exploitation crimes," such as the ones noted in the affidavit. *Id.* ¶ 10. It further stated that the "administrators and users of the TARGET WEBSITE regularly send and receive illegal child pornography via the website." *Id.* The NIT Affidavit also described the massive scale of the site, which appeared to have been operating since August 2014; site statistics indicated that, as of February 3, 2015, it contained 158,094 members, 9,333 message threads, and 95,148 posted messages. *Id.* ¶ 11.

The NIT Affidavit explained that the Playpen website was a global online forum dedicated to the advertisement and distribution of child pornography through which registered users regularly advertised, distributed, and accessed child pornography. The scale of child sexual exploitation material exchanged on the Playpen website was massive – the website had 150,000 members who collectively engaged in tens of thousands of postings related to child pornography. The images and videos that were advertised, distributed, and accessed through the

website were categorized according to gender, and age of the victims portrayed, including so-called "jailbait," "pre-teen," and "toddlers," as well as the type of sexual activity depicted, including hardcore ("HC") and softcore ("SC") child pornography. The most posts to the site (more than 20,000 posts) were made within the subsection "Pre-teen" videos dubbed "Girls HC," where hardcore pornographic images of pre-teen girls were advertised, distributed, and accessed by Playpen members. Playpen also contained forums for the discussion of matters pertinent to the sexual abuse of children, including methods and tactics offenders exchanged concerning abusing children as well as methods offenders use to avoid detection of their illegal activities by law enforcement authorities while perpetrating online child sexual exploitation crimes. Playpen did not advertise or distribute adult pornography.

Playpen operated on the anonymous Tor network, which allows users to hide their actual IP addresses while accessing the Internet. In order to access the Tor network, a user must install Tor software by either downloading the "add-on" to the user's web browser or by downloading the free "Tor browser bundle" available at www.torproject.org. Use of the Tor software "anonymizes" the user's IP address by routing user communications around a network of relay computers (called "nodes") operated by volunteers all around the world. Because of the way Tor routes communications through other computers, the techniques typically used by law enforcement to identify the IP address of an offender are thwarted because the "exit node" to a website accessed by a Tor user would be the IP address, rather than the user's IP address, would be discoverable on the IP log from the accessed website. In this way it is impossible to trace the user's actual IP address back through the nodes of the Tor network to the user's IP address.

Within the Tor network itself, entire websites such as Playpen can be set up as "hidden services." "Hidden services," are hosted on computer servers that communicate through IP

addresses and operate the same as regular public websites with one important exception: the IP address for the web server is hidden and instead replaced with a Tor-based web address, which is a series of algorithm-generated alpha numeric characters followed by the suffix ".onion." A user can only reach these "hidden services" if the user is using the Tor client software and operating in the Tor network. Unlike an open Internet website, it is not possible to determine through public lookups the IP address of the computer hosting the Tor "hidden service." Neither law enforcement nor users can therefore determine the location of the computer that hosts the website through those public lookups.

The use of the Tor network makes websites like Playpen more difficult for users to find. Even after connecting to the Tor network, a user must know the exact web address of a site like Playpen in order to access it. Accordingly, in order to find a site like Playpen, a user must first obtain the web address from another source, such as from others familiar with the website or from online postings describing the sort of content available and its web address. Accessing a Tor website like Playpen therefore requires several affirmative steps by the user, making it extremely unlikely that a person simply stumbled upon the website without first understanding the content and purpose of the website.

While the FBI was able to view and document the substantial illicit activity taking place on Playpen, investigators faced a tremendous challenge to identify Playpen users engaging in sexual exploitation of children through the site. Open-Internet, non-Tor websites generally have user IP address logs that can be used to locate and identify the website's users. Law enforcement agents could then perform a publicly available lookup to determine what Internet Service Provider ("ISP") owned the target IP address, and issue a subpoena to the ISP to determine the user to which the IP address had been assigned on the relevant date and time. However, because

Playpen was a Tor website, any such logs of user activity would contain only the IP address of the last computer through which the communications of Playpen's users were routed (the "exit node") before the communications reached Playpen. The exit node is not the computer of the user who was intentionally accessing Playpen; therefore, it is normally not possible to trace such communications back to the Playpen user. Such IP address logs therefore could not be used to identify and locate Playpen users like the defendant. Accordingly, in order for law enforcement to be able to attain the sort of information that would identify the users through the ordinary investigative means, the offenders' use of the Tor network necessitated a particular investigative strategy.

Acting on a tip from a foreign law enforcement agency as well as further FBI investigation, the FBI determined that the computer used to host Playpen was located at a web-hosting facility in North Carolina. In February of 2015, FBI agents apprehended the administrator of Playpen and seized the web-hosting facility in North Carolina. Rather than merely shutting the site down, which would have allowed the Playpen users to go unidentified, the FBI interdicted the site and allowed it to continue to operate at a government facility located in the Eastern District of Virginia during a two-week period between February 20, 2015 and March 4, 2015. During that period, the FBI obtained court approval from the United States District Court for the Eastern District of Virginia ("EDVA") to monitor site users' communication and deploy a NIT on the site in order to attempt to identify registered site users who were anonymously engaging in the continuing sexual abuse and exploitation of children, and to locate and rescue children from the imminent harm of ongoing abuse and exploitation. As described in detail in the application for the warrant authorizing its use, the NIT consisted of computer instructions which, when downloaded along with other content of Playpen by a

registered user's computer, were designed to cause the user's computer to transmit a limited set of information – the user's true IP address and other computer-related information – that would assist in identifying the computer used to access Playpen and its user. (Attachment 1, ¶¶ 31-37.) The search warrant authorization permitted that minimally invasive technique to be deployed when a registered user logged into Playpen by entering a username and password while the website was being hosted in the EDVA. Playpen user "Teddybear555's" computer's IP address was identified as operating from the defendant's residence.

A federal search warrant was obtained for the defendant's residence on October 15, 2015. The affidavit in support of the warrant for the defendant's residence described Playpen in detail[1] and articulated that data obtained from logs on Playpen, court-authorized monitoring by law enforcement, and the court-authorized deployment of the NIT had revealed that Playpen user "Teddybear555" had been logged onto the Playpen website for 20 hours between February 26, 2015, through March 4, 2015. Affidavit of SA Kristina Norris (Doc. 14-3)(hereinafter "Norris Affidavit") ¶ 30. The affidavit further detailed various posts or discussions which "Teddybear555" had accessed during that period, including posts entitled "Man and Girl Cum," a post linking an image of a prepubescent male child fellating an adult male and a post linking a depiction of a prepubescent male minor fellating another prepubescent male minor. Norris Affidavit ¶¶ 31-35. The NIT revealed the IP address of "Teddybear555" and a subpoena was issued to the ISP that operated that IP address. The information obtained from the subpoena revealed that the IP address used by "Teddybear555" was assigned to the defendant's residence.

[1] In order to preserve the ongoing investigations, the affidavit in support of the warrant for the defendant's residence described Playpen as "Website A." (*See* Affidavit at Footnotes 1 and 2.)

Law enforcement officers executed the federal search warrant for the defendant's residence on October 20, 2015 and searched the defendant's residence and seized a laptop computer with an internal hard drive. A forensic examination of the hard drive revealed the presence of child pornography, as well as the installation of the Tor software. The defendant was indicted on March 8, 2016.

Contrary to the defendant's suggestion that Playpen was not *per se* illegal, as set out in the NIT Affidavit, the illicit purpose of Playpen was immediately apparent to any user who was able to find the site. As the Affiant explained, "on the main page of the site, located to either side of the site name were two images of partially clothed prepubescent females with their legs spread apart." *Id.* ¶ 12. The combination of the prepubescent images along with terms of art describing preferred methods for posting images unmistakably marked Playpen as a hub for trafficking illicit child pornography on a massive scale. *See, id.* ¶ 12. This was certainly heavily buttressed by the information provided in Special Agent Norris' Affidavit in support of the warrant for defendant Scarbrough's residence, described above.

The NIT Affidavit also explained that Playpen users were required to register an account by creating a username and password before they could access the site. Users who chose to register were required to accept terms of registration, the entire text of which is included in the NIT Affidavit. The registration text repeatedly warned prospective users to be vigilant about their security and potential to be identified, stating that "the forum operators do NOT want you to enter a real [email] address," that users "should not post information [in their profile] that can be used to identify you," that "it is impossible for the staff or owners of this forum to confirm the true identity of users," that "[t]his website is not able to see your IP," and that "[f]or your own security, when browsing on Tor we also recommend [sic] that you turn off javascript and disable

sending the 'referer' header." *Id.* ¶ 13. The repeated security warnings of site administration within those registration terms further reflect that Playpen was a facility for illicit activity.

## II. Argument[2]

Defendant asserts that it was beyond the authority of the United States Magistrate Judge who issued the NIT warrant, in that it supposedly exceeded the jurisdictional limits under Rule 41[3] of the Federal Rules of Criminal Procedure for a judicial official in the Eastern District of

[2] Defendant wholly fails to explain what or how any First Amendment right he may have had was abridged by the NIT Warrant or search warrant for the defendant's residence in this case. Further, he fails to explain what protected speech has been abridged by the NIT Warrant or his prosecution in this case; therefore, the United States respectfully submits that the evidence should not be suppressed on the basis of the First Amendment argument he advances in his Motion.

[3] Federal Rule of Criminal Procedure 41(b) provides in relevant part:
(b) Authority to Issue a Warrant. At the request of a federal law enforcement officer or an attorney for the government:
(1) a magistrate judge with authority in the district -- or if none is reasonably available, a judge of a state court of record in the district -- has authority to issue a warrant to search for and seize a person or property located within the district;
(2) a magistrate judge with authority in the district has authority to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed;
(3) a magistrate judge--in an investigation of domestic terrorism or international terrorism--with authority in any district in which activities related to the terrorism may have occurred has authority to issue a warrant for a person or property within or outside that district;
(4) a magistrate judge with authority in the district has authority to issue a warrant to install within the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both; and
(5) a magistrate judge having authority in any district where activities related to the crime may have occurred, or in the District of Columbia, may issue a warrant for property that is located outside the jurisdiction of any state or district, but within any of the following:
(A) a United States territory, possession, or commonwealth;
(B) the premises--no matter who owns them--of a United States diplomatic or consular mission in a foreign state, including any appurtenant building, part of a building, or land used for the mission's purposes; or
(C) a residence and any appurtenant land owned or leased by the United States and used by United States personnel assigned to a United States diplomatic or consular mission in a foreign state.

Virginia to authorize the NIT to obtain information from the defendant's computer in the Eastern District of Tennessee.

The Sixth Circuit has explained "[a]lthough the purpose of Rule 41 is the implementation of the Fourth Amendment, the particular procedures it mandates are not necessarily part of the Fourth Amendment." *United States v. Searp*, 586 F.2d 1117, 1121 (6th Cir. 1978), *cert. denied* 440 U.S. 921 (1979). Even where there is a failure to comply with Rule 41, a search may nevertheless be "reasonable" in the constitutional sense and meet the requirements of the Fourth Amendment. *Id*. at 1122. For this reason, the Sixth Circuit has instructed that "[v]iolations of Rule 41 alone should not lead to exclusion unless (1) there was 'prejudice' in the sense that the search might not have occurred or would not have been so abrasive if the Rule had been followed, or (2) there is evidence of intentional and deliberate disregard of a provision in the Rule." *Id.* at 1125 (quoting *United States v. Burke*, 517 F.2d 377, 386-87 (2d Cir.1975)).

**A. Rule 41 and the Fourth Amendment Do Not Support Suppression of the Evidence.**

In *United States v. Michaud*, 2016 WL 337263 (W.D. Wash. Jan. 28, 2016), the court denied a motion to suppress. The defendant in *Michaud* raised two Fourth Amendment arguments: whether deploying the NIT from the Eastern District of Virginia, to the defendant's computer, located outside that district, exceeded the scope of the NIT warrant's authorization; and whether the NIT warrant lacks particularity and amounts to a general warrant. Id. at *3. The defendant also argued that the NIT warrant violated Federal Rule of Criminal Procedure 41(b). As to the first argument, regarding the scope of the NIT warrant, the court explained: "Whether a search or seizure exceeds the scope of a warrant is an issue that is determined 'through an objective assessment of the circumstances surrounding the issuance of the warrant, the contents

of the search warrant, and the circumstances of the search.'" *Id*. at *3 (quoting *U.S. v. Hurd*, 499 F.3d 963, 966 (9th Cir. 2007)). The court explained that "while the NIT Warrant cover sheet does explicitly reference the Eastern District of Virginia, that reference should be viewed within context." *Id*. at *4.6. The court explained that in the blank space on the warrant where the magistrate judge is to "give its location," the blank has been filled in with "See Attachment A." *Id*. The court explained further that:

> Attachment A, subtitled "Place to be Searched," authorizes deployment of the NIT to "all activating computers," defined as "those of any user or administrator who logs into [Website A] by entering a username and password." *Id*. Attachment A refers to the Eastern District of Virginia as the location of the government-controlled computer server from which the NIT is deployed. *Id*. A reasonable reading of the NIT Warrant's scope gave the FBI authority to deploy the NIT from a government-controlled computer in the Eastern District of Virginia against anyone logging onto Website A, with any information gathered by the NIT to be returned to the government-controlled computer in the Eastern District of Virginia.

*Id.* The court explained that the warrant application reinforces the objectively reasonable interpretation because when detailing how the NIT works, the warrant application explains that the NIT "may cause an activating computer—*wherever located*—to send to a computer controlled by or known to the government [in the Eastern District of Virginia], *network level messages containing information that may assist in identifying the computer, its location*, and other information[.]" *Id*. (emphasis added).

As to the argument that the NIT warrant lacks particularity and amounts to a general warrant, the court explained that whether a warrant lacks specificity depends on two factors: particularity and breadth. *Id*. (citing *United States v. SDI Future Health, Inc*., 568 F.3d 684, 702 (9th Cir. 2009)). The court concluded that the NIT warrant was not lacking in particularity and did not exceed the breadth—or scope—of the probable cause on which it was based. *Id*. at *5. The court also concluded that even if the NIT Warrant was unconstitutional because it is a

general warrant, suppression may not be required under *United States v. Leon*, 468 U.S. 897 (1984) because the officers were acting in good faith when executing the warrant. *Id*.

As to the argument that the NIT warrant violates Rule 41(b), the court found that the NIT technically violated the letter, but not the spirit of the rule. *Id*. The court explained: "The rule does not directly address the kind of situation that the NIT Warrant was authorized to investigate, namely, where criminal suspects geographical whereabouts are unknown, perhaps by design, but the criminal suspects had made contact via technology with the FBI in a known location." *Id*. at *6. The court explained that because there was a technical violation of the Rule, and not a violation of a constitutional magnitude: "courts may suppress where a defendant suffers prejudice, 'in the sense that the search would not have occurred...if the rule had been followed,' or where law enforcement intentionally and deliberately disregarded the rule." *Id*. (quoting *United States v. Weiland*, 420 F.3d 1062, 1071 (9th Cir. 2005)). The court clarified that "prejudice" meant considering "whether the evidence obtained from a warrant that violates Rule 41(b) could have been available by other lawful means." *Id*. (citing *United States v. Vasser*, 648 F.2d 507, 511 (9th Cir. 1980)). The court found that the defendant did not suffer prejudice:

> Mr. Michaud has no reasonable expectation of privacy of the most significant information gathered by deployment of the NIT, Mr. Michaud's assigned IP address, which ultimately led to Mr. Michaud's geographic location. *See United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008). Although the IP addresses of users utilizing the Tor network may not be known to websites, like Website A, using the Tor network does not strip users of all anonymity, because users accessing Website A must still send and receive information, including IP addresses, through another computer, such as an Internet Service Provider, at a specific physical location. Even though difficult for the Government to secure that information tying the IP address to Mr. Michaud, the IP address was public information, like an unlisted telephone number, and eventually could have been discovered.

*Id*. at *7. The court also found that the FBI did not act intentionally and with deliberate disregard of Rule 41(b). *Id*. Therefore, the court found that even if the NIT warrant was invalid,

the FBI executed the warrant in good faith under *United States v. Leon*, 468 U.S. 897 (1984). *Id*. Accordingly, the court denied the defendant's motions to suppress. *Id*. at *8.

Likewise in *United States v. Werdene,*[4] the United States District Court for the Eastern District of Pennsylvania denied the defendant's motion to suppress based upon the NIT warrant. The court surveyed the cases that have dealt with the NIT warrant and summarized:

> Although the courts generally agree that the magistrate judge in Virginia lacked authority under Rule 41 to issue the warrant, they do not all agree that suppression is required or even appropriate. *Compare Michaud*, 2016 WL 337263, at *6–7 (finding violation of Rule 41(b) but suppression unwarranted because defendant was not prejudiced and FBI agents acted in good faith), *and Epich*, 2016 WL 953269, at *2 (rejecting Defendant's contention that Rule 41 was violated and finding suppression unwarranted even if it was), *with Levin*, 2016 WL 2596010, at *7–15 (finding suppression warranted because Rule 41 "implicates substantive judicial authority," Defendant was prejudiced even if the violation was technical, and the good faith exception to the exclusionary rule is not available because the warrant was void *ab initio*), *and Arterbury*, slip op. at 13–29 (same).

After finding that the NIT warrant was not specifically authorized by Rule 41(b), the *Werdene* court nevertheless declined to suppress evidence seized on a search warrant predicated on the results of the NIT warrant. The court noted that the defendant could not claim a reasonable expectation of privacy in the identity of his IP address. *Id* at *16 – 17 (citations omitted). According to the court, any actual, subjective expectation of privacy held by Werdene was not legitimate. *Id.* at *20. Further, the court noted that the NIT Warrant was approved by a neutral and detached magistrate judge and based upon "copious detail" set out in the NIT

[4] 2:15-cr-004340-GJP (E.D.Pa May 19, 2016) The *Weredene* court listed the most recent cases addressing the issue: *United States v. Levin*, 15-cr-10271, 2016 WL 2596010 (D. Mass. May 5, 2016); *United States v. Arterbury*, 15-cr-182 (N.D. Okla. Apr. 25, 2016) (report and recommendation); *United States v. Epich*, 15-cr-163, 2016 WL 953269 (E.D. Wis. Mar. 14, 2016); *United States v. Stamper*, No. 15-cr-109 (S.D. Ohio Feb. 19, 2016); *United States v. Michaud*, 15-cr-05351, 2016 WL 337263 (W.D. Wash. Jan. 28, 2016).

Affidavit. *Id.* at 21-22. As such, the *Werdene* court concluded that the violation of Rule 41(b) was "non-constitutional" and did not prejudice the defendant. *Id.*

In *United States v. Stamper,* District Judge Michael R. Barrett denied a motion to suppress evidence obtained based on a search warrant predicated on information obtained via the NIT Warrant, based upon the reasoning set forth in *Michaud*. Judge Barrett held that, despite the fact that the warrant technically violated Rule 41(b), the defendant suffered no prejudice, the defendant had no legitimate expectation of privacy in his IP address to support the defendant's Fourth Amendment argument, and there was no evidence of intentional and deliberate violation of Rule 41(b) by law enforcement. *Stamper* at *22-23.

Likewise, there is no evidence of intentional and deliberate disregard of Rule 41(b) by the government here. The government specifically requested the NIT warrant authorizing the NIT to cause an activating computer-*wherever located*-to send to a computer controlled by or known to the government, network level messages containing information that may assist in identifying the computer, its location, other information about the computer and the user of the computer. NIT Affidavit ¶ 46. Therefore, even if the NIT Warrant technically violates rule 41(b), exclusion is unnecessary.

**B. *Leon* Good Faith Exception Overrides Any Technical Violation of Rule 41(b).**

Simply because a technical violation of Rule 41(b) and the Fourth Amendment may have occurred, it does not necessarily follow that the evidence obtained should be excluded, which is a remedy of last result. It is only when the deterrent value to law enforcement exceeds the substantial social cost of exclusion of evidence that exclusion of the evidence is warranted. A magistrate judge's mistaken belief that she has jurisdiction to issue a warrant, absent any indicia of intentional wrongdoing or reckless conduct by the agents, does not warrant suppression of

evidence. Exclusion of evidence in this case would serve only to punish errors of judges and magistrates without an appreciable effect on law enforcement. *United States v. Leon*, 468 U.S. 897, 909, 916 (1984). Here, the affiant for the NIT clearly explained the techniques to be employed and the methods by which the FBI expected to obtain the information concerning the IP addresses from the NIT. Once issued, the agents acted upon an objectively reasonable good faith belief of the legality of their conduct. Suppression of the evidence in the case of defendant Scarbrough cannot logically contribute to deterrence of Fourth Amendment violations occasioned by a magistrate's error of the scope or breadth of her authority to issue the NIT Warrant. *Id.* at 921.[5]

## III. CONCLUSION

For the foregoing reasons, the United States respectfully submits that the Court should deny the defendant's Motion.

Respectfully submitted this 23rd day of May, 2016.

NANCY STALLARD HARR
ACTING UNITED STATES ATTORNEY

By: *s/ Matthew T. Morris*
Matthew T. Morris
Assistant United States Attorney
800 Market Street, Suite 211
Knoxville, Tennessee 37902
(865) 545-4167

[5] The United States would point out that the District of Massachusetts has suppressed evidence obtained on a warrant predicated on the results of the NIT Warrant. *United States v. Levin,* No. 15-10271-WGY (D. Mass. Mar. 20, 2016). (*See also*, *United States v. Arterbury*, No. 15-CR-182-JHP (N.D.Okla April 15, 2016). In *Levin*, the court found that *Leon* did not permit the usage of evidence based upon a warrant that void *ab initio* because it exceeded the issuing magistrate's authority. However, the *Levin* court noted that, within the Sixth Circuit, *Leon* can be extended to warrants that were issued outside of a magistrate's authority, citing *United States v. Master,* 614 F.3d 236, 242 (6th Cir. 2010).

**CERTIFICATE OF SERVICE**

I hereby certify that on May 23, 2016, the foregoing was filed electronically. Notice of this filing will be sent by operation of the Court's electronic filing system to all parties indicated on the electronic filing receipt. Parties may access this filing through the Court's electronic filing system.

By: *s/ Matthew T. Morris*
Matthew T. Morris
Assistant United States Attorney